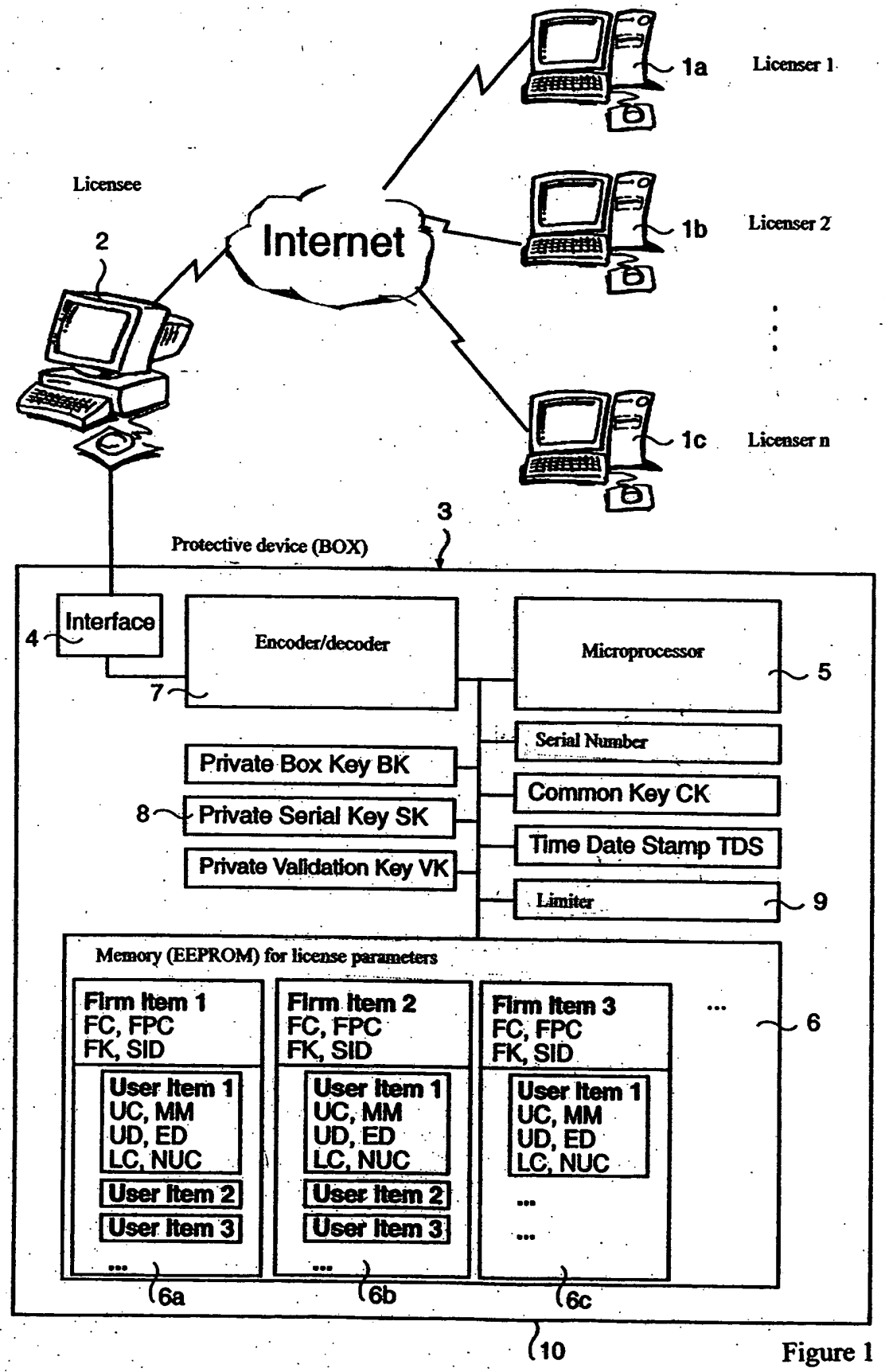
Licensee
2
Internet
1a
Licenser 1
1b
Licenser 2
1c
Licenser n
3
Protective device (BOX)
Interface
4
Encoder/decoder
7
Microprocessor
5
Serial Number
Private Box Key BK
Common Key CK
8
Private Serial Key SK
Time Date Stamp TDS
Private Validation Key VK
Limiter
9
Memory (EEPROM) for license parameters
Firm Item 1
FC, FPC
FK, SID
Firm Item 2
FC, FPC
FK, SID
Firm Item 3
FC, FPC
FK, SID
6
User Item 1
UC, MM
UD, ED
LC, NUC
User Item 2
User Item 3
6a
6b
6c
10

Figure 1

Keys and data at the producer

Common Key (CK), calculated therefrom Firm Common Key (FCK)
Box Key (BK), makes available Public Box Key
Validation Key (VK)

Figure 2a

Keys and data at the licenser

Firm Code (FC)
Firm Common Key (FCK)
Firm Key (FK)
Box Key (BK)

Figure 2b

Keys and Data at the Licensee

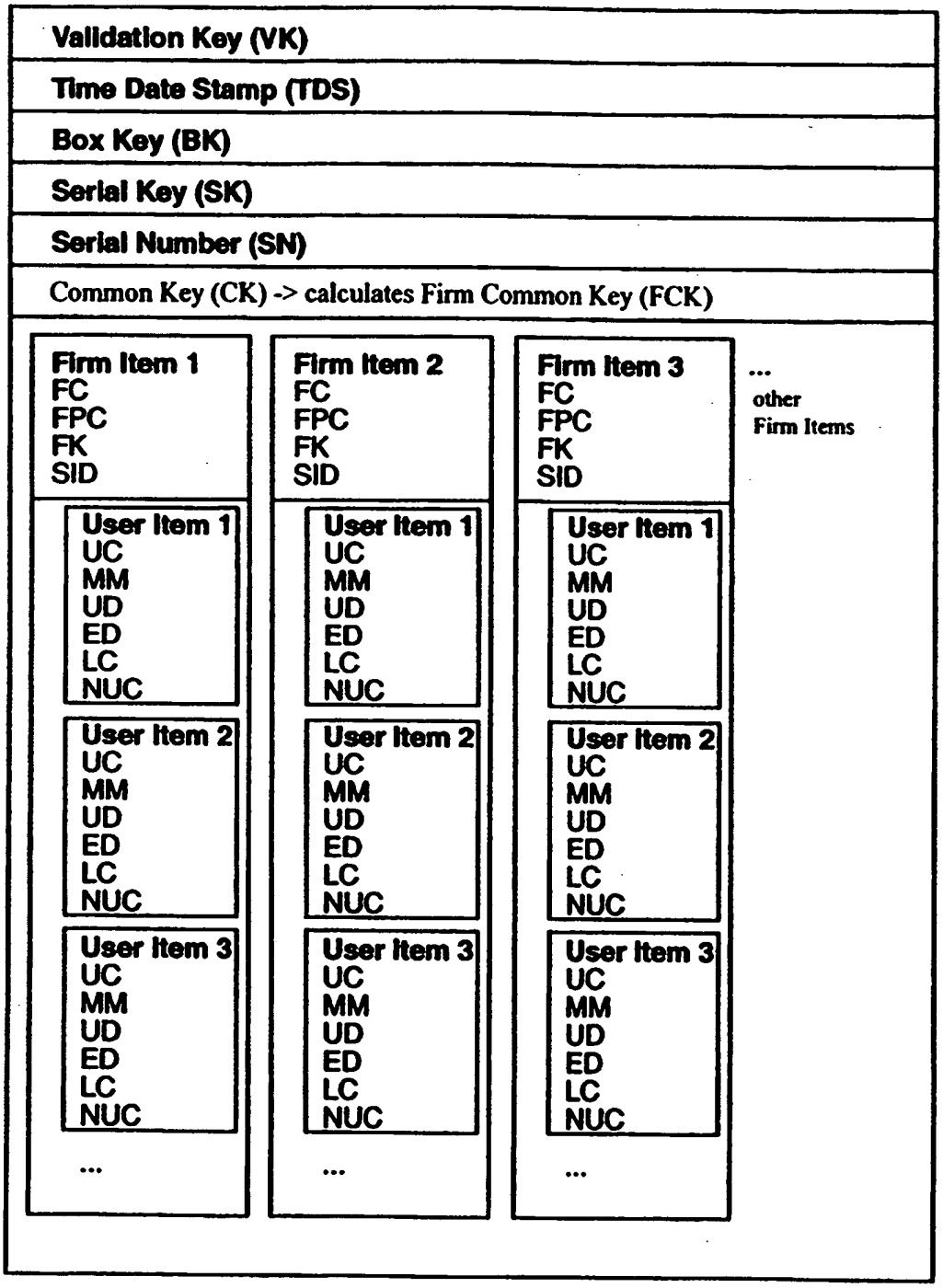

Fig. 3

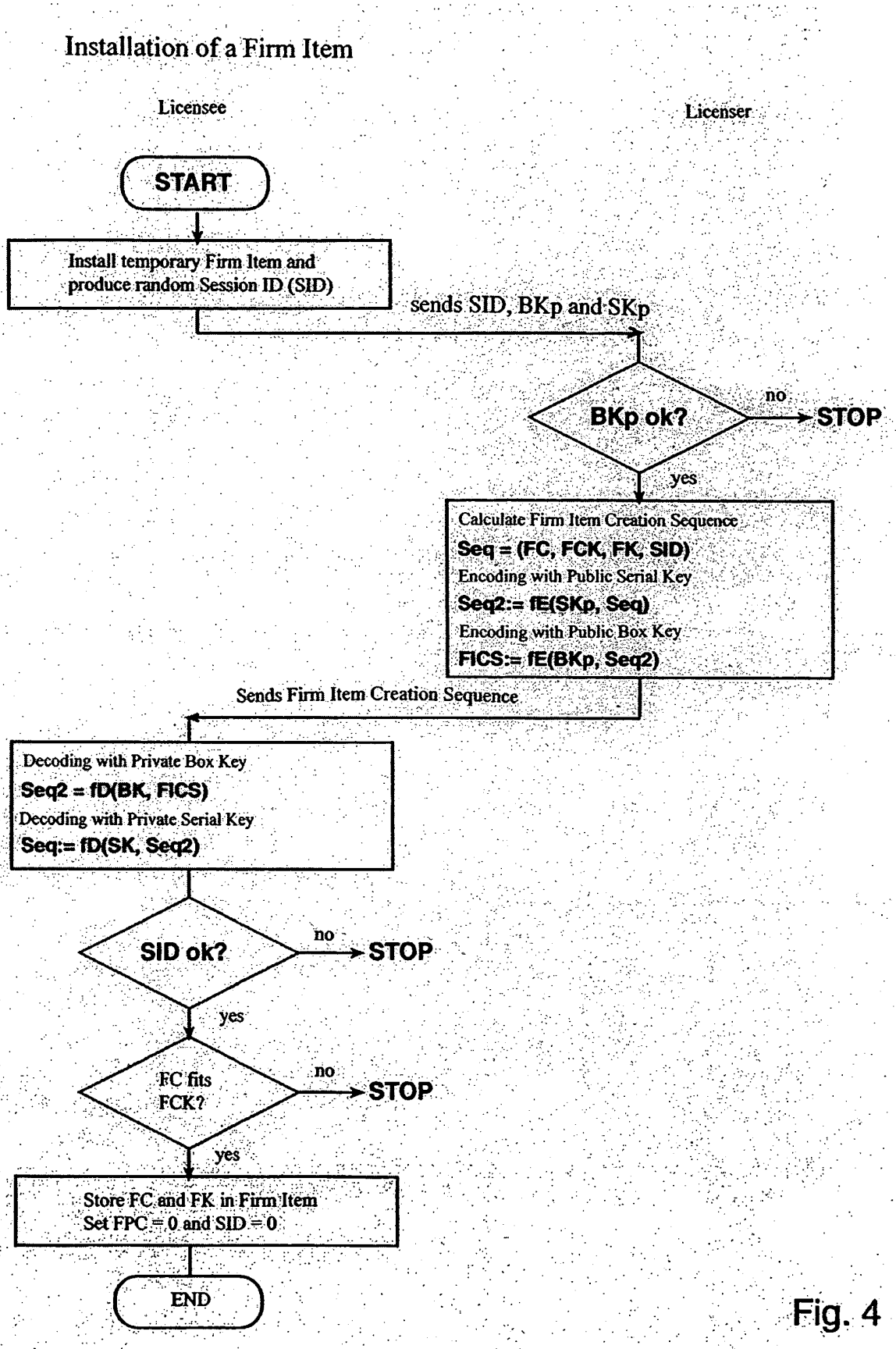
Installation of a Firm Item
Licensee
Licenser
START
Install temporary Firm Item and produce random Session ID (SID)
sends SID, BKp and SKp
BKp ok?
no
STOP
yes
Calculate Firm Item Creation Sequence
Seq = (FC, FCK, FK, SID)
Encoding with Public Serial Key
Seq2:= fE(SKp, Seq)
Encoding with Public Box Key
FICS:= fE(BKp, Seq2)
Sends Firm Item Creation Sequence
Decoding with Private Box Key
Seq2 = fD(BK, FICS)
Decoding with Private Serial Key
Seq:= fD(SK, Seq2)
SID ok?
no
STOP
yes
FC fits FCK?
no
STOP
yes
Store FC and FK in Firm Item
Set FPC = 0 and SID = 0
END

Fig. 4

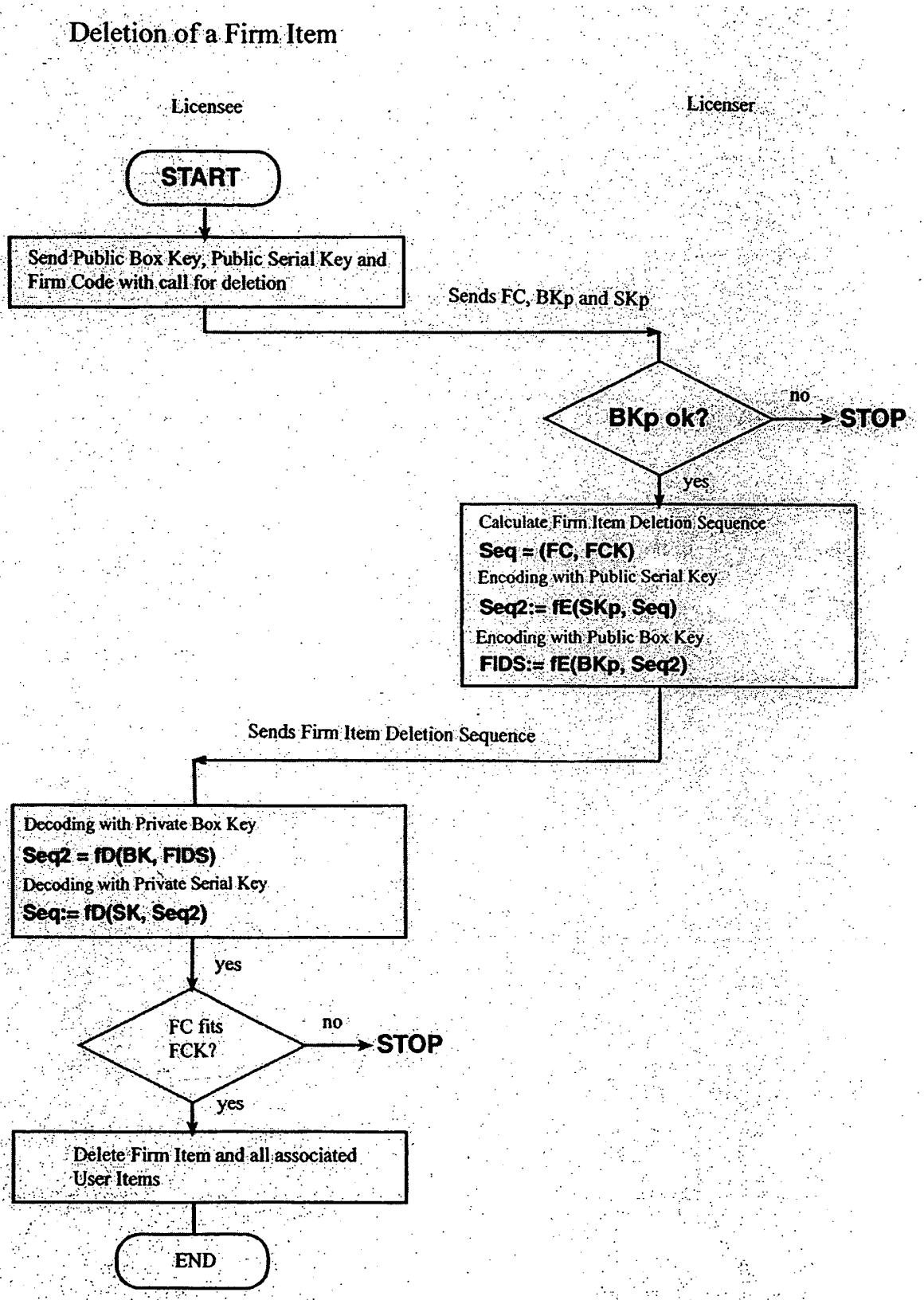
Deletion of a Firm Item
Licensee
Licenser
START
Send Public Box Key, Public Serial Key and Firm Code with call for deletion
Sends FC, BKp and SKp
BKp ok?
no
STOP
yes
Calculate Firm Item Deletion Sequence
Seq = (FC, FCK)
Encoding with Public Serial Key
Seq2:= fE(SKp, Seq)
Encoding with Public Box Key
FIDS:= fE(BKp, Seq2)
Sends Firm Item Deletion Sequence
Decoding with Private Box Key
Seq2 = fD(BK, FIDS)
Decoding with Private Serial Key
Seq:= fD(SK, Seq2)
yes
FC fits FCK?
no
STOP
yes
Delete Firm Item and all associated User Items
END

Fig. 5

Installation, Modification, or Deletion of a User Item

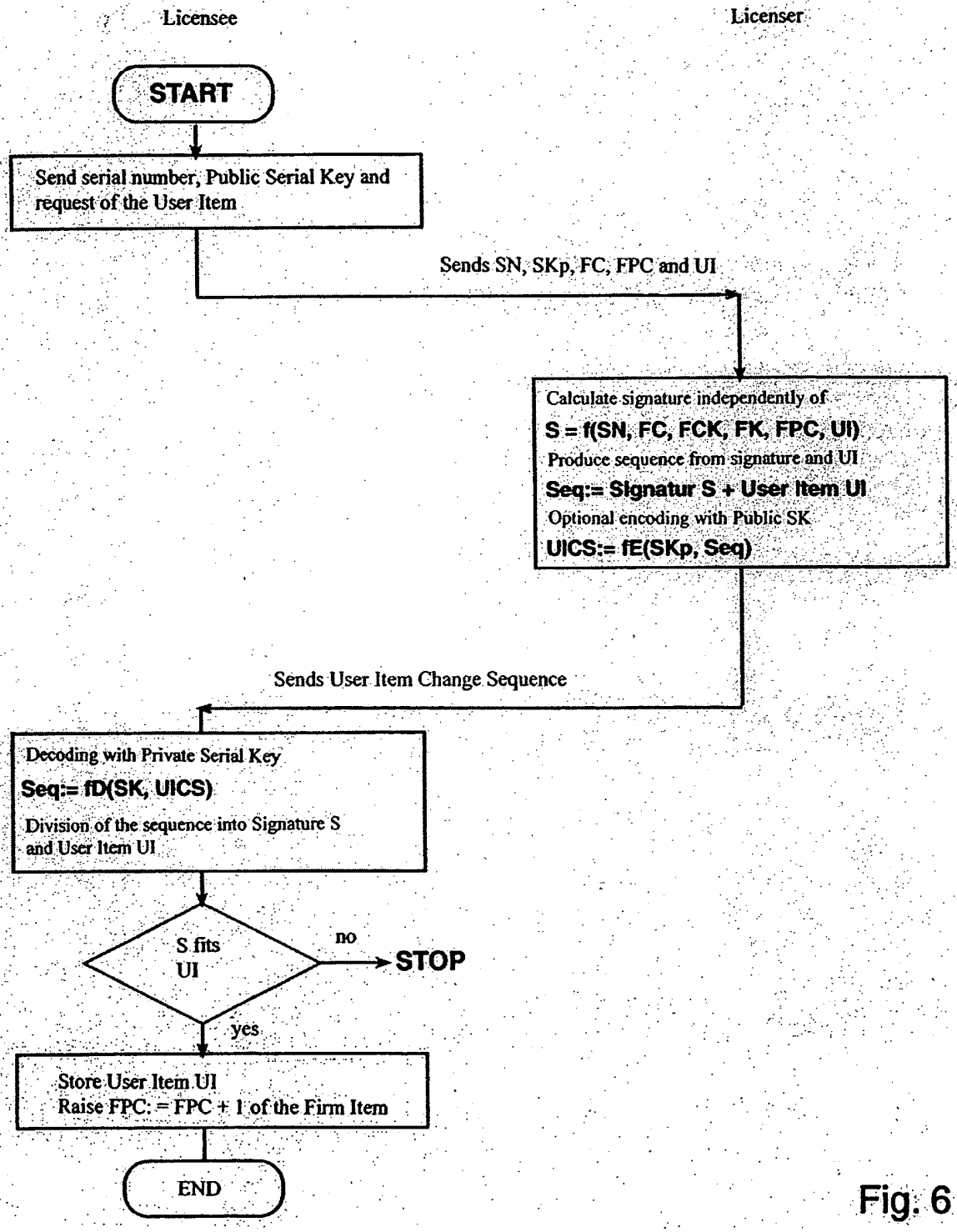

Fig. 6

Initializing of a Decoding

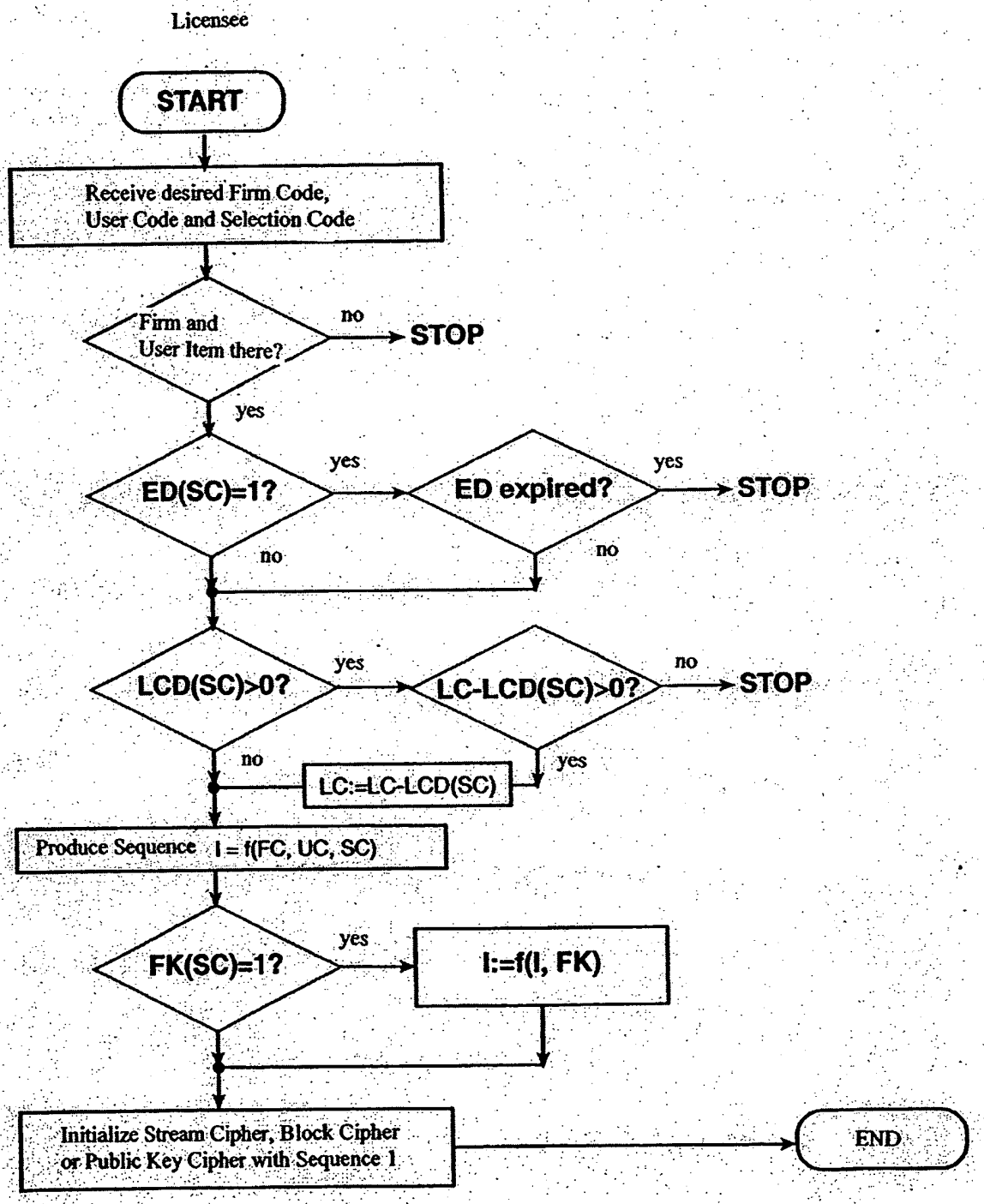

Fig. 7

Setting of a Time Date Stamp TDS of Reference Source

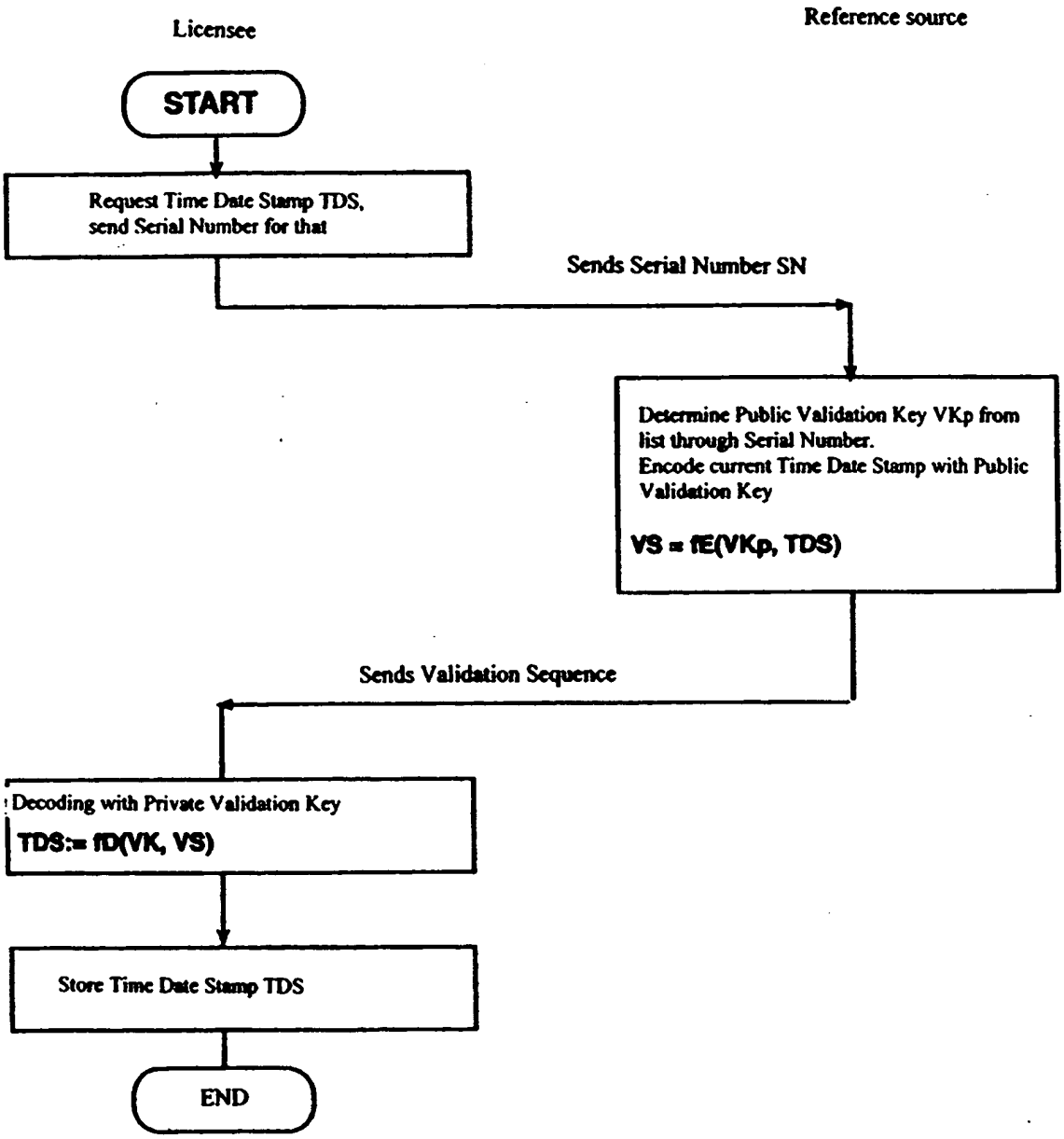

Fig. 8